



## PATENT ABSTRACTS OF JAPAN

(11) Publication number: **11068730 A**

(43) Date of publication of application: 09 . 03 . 99

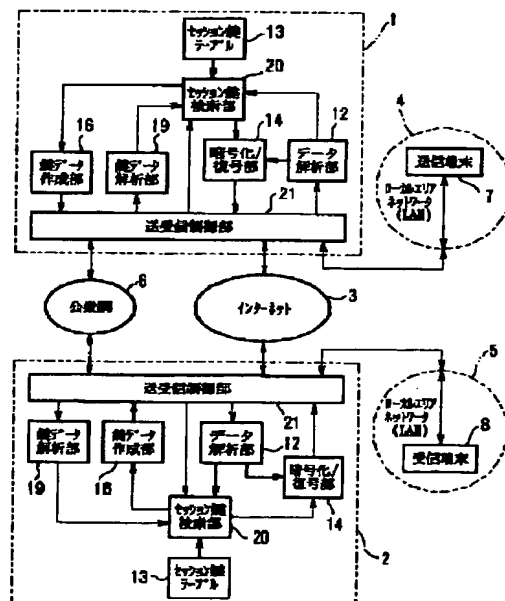
(51) Int. Cl.

**H04L 9/08****H04L 9/10****H04L 12/46****H04L 12/28****H04L 12/66**(21) Application number: **09220478**(22) Date of filing: **15 . 08 . 97**(71) Applicant: **NEC COMMUN SYST LTD**(72) Inventor: **ONO SEIJI****(54) ENCRYPTION GATEWAY DEVICE****(57) Abstract:**

**PROBLEM TO BE SOLVED:** To provide an encryption gateway device by which encryption communication with high security is realized without giving effect on the hardware and the application program of an existing terminal.

**SOLUTION:** Encryption gateway devices 1, 2 are placed on a border between local area networks 4, 5 and the internet 3 and encrypted data are transferred only through the internet 3 and key data are transferred through a route of a public network 6. Since the encrypted data and key data to decode the encryption are transferred through the routes physically different from each other, communication with high security is realized and since the encryption data are communicated without special revamping of a destination terminal, the cost increase to secure the confidentiality is minimized.

COPYRIGHT: (C)1999,JPO



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-68730

(43) 公開日 平成11年(1999) 3月9日

(51) Int.Cl.<sup>6</sup>

識別記号

F I

H 0 4 L 9/08  
9/10  
12/46  
12/28  
12/66

H 0 4 L 9/00

6 0 1 B

6 0 1 E

6 2 1 A

3 1 0 C

11/00

11/20

B

審査請求 有 請求項の数 3 O L (全 8 頁)

(21) 出願番号

特願平9-220478

(22) 出願日

平成9年(1997) 8月15日

(71) 出願人 000232254

日本電気通信システム株式会社  
東京都港区三田1丁目4番28号

(72) 発明者 小野 誠司

東京都港区三田1丁目4番28号 日本電気  
通信システム株式会社内

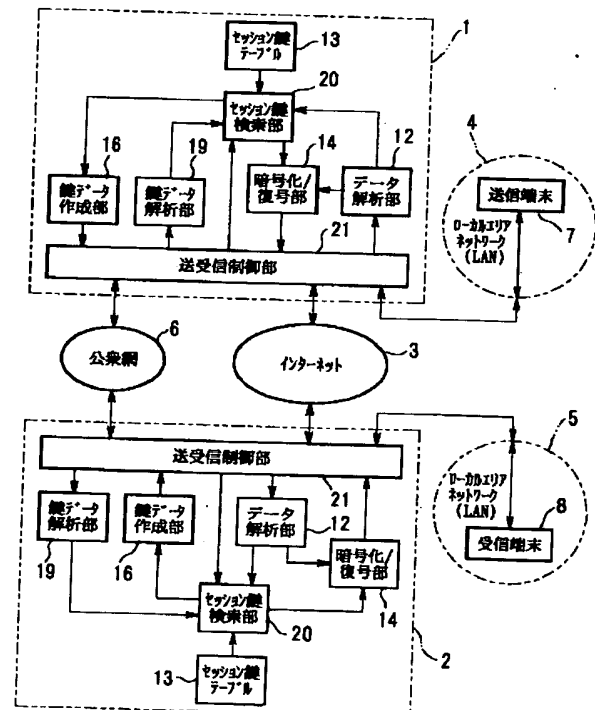
(74) 代理人 弁理士 志賀 正武

(54) 【発明の名称】 暗号ゲートウェイ装置

(57) 【要約】

【課題】 既存の端末のハードウェア及びアプリケーションプログラムに影響を与えることなく機密性の高い暗号化通信を実現する暗号ゲートウェイ装置を提供する。

【解決手段】 ローカルエリアネットワーク4、5とインターネット3の境界に暗号ゲートウェイ装置1、2を置き、インターネット3を通る間だけ暗号化したデータにて転送を行い、鍵データは公衆網6のルートで転送する。これにより、暗号化データと、その暗号を解くための鍵データとが物理的に異なるルートで転送されるので、機密性の高い通信を実現でき、また送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。



## 【特許請求の範囲】

【請求項1】 送信端末からの情報を受信し、その受信情報の暗号化／復合を行う暗号ゲートウェイ装置であって、

送信端末及び受信端末の識別情報と暗号化又は復合のためのセッション鍵の組を保持するセッション鍵テーブルと、

このセッション鍵テーブルから該当するセッション鍵を検索するセッション鍵検索手段と、

暗号化を行うための確認データ等を送受信するデータ送信手段及びデータ受信手段と、

暗号データや確認データ等を解析するデータ解析手段と、

受信した暗号化データ又は通常データを暗号化又は復合する暗号化／復合手段と、

暗号化を解く鍵データをダイヤルアップ等により別ルートにて受け渡しするための鍵データ送信手段及び鍵データ受信手段と、

受信した鍵データを解析する鍵データ解析手段と、

セッション鍵検索の結果で鍵データを作成する鍵データ作成手段と、

を備え、

ユーザからの暗号化指示により、暗号化データと鍵データを物理的に別ルートで転送することを特徴とする暗号ゲートウェイ装置。

【請求項2】 前記暗号化データをインターネットを使用して転送し、前記鍵データを公衆網を使用して転送することを特徴とする請求項1記載の暗号ゲートウェイ装置。

【請求項3】 前記暗号化データをインターネットを使用して転送し、前記鍵データを専用回線を使用して転送することを特徴とする請求項1記載の暗号ゲートウェイ装置。

## 【発明の詳細な説明】

## 【0001】

【発明の属する技術分野】本発明は、暗号ゲートウェイ装置に係り、特に広範囲に分散した事業所間をインターネットを介して暗号化通信を行う暗号ゲートウェイ装置に関する。

## 【0002】

【従来の技術】図6は従来の暗号通信システムの構成を示すブロック図である。この図において、端末130と端末140との間で通信を行う場合、一方の端末130のアプリケーションプログラム132（以下、APと略す）が鍵配送センタ160より通信に使用するセッション鍵162を取得する。端末130のAP132は、このセッション鍵を通信相手の端末140に送信することで2台の端末130、140で共通のセッション鍵を共有し、このセッション鍵を用いて通信文を暗号化及び復合して暗号通信を行う。

【0003】図7は従来の暗号ゲートウェイ装置180の構成を示すブロック図である。この図において、暗号ゲートウェイ装置180は、暗号化／復合を行うための固定セッション鍵181と、受信情報を受信するための受信部182と、受信情報を解析して通信文を抽出する受信情報解析部183と、固定セッション鍵181を利用して通信文を暗号化／復合する暗号化／復合部184と、暗号化／復合された通信文を送信する送信部185とから成る。

【0004】図8は図7に示す暗号ゲートウェイ装置180を利用した暗号通信システムの構成を示すブロック図である。この図において、端末21-1、21-2、…、21-mから成るAグループの端末に暗号ゲートウェイ装置180-1が外付けされ、また端末31-1、31-2、…、31-nから成るBグループの端末に暗号ゲートウェイ装置180-2が外付けされる。暗号ゲートウェイ装置180-1、180-2のセッション鍵は固定であるため、端末21-1と31-2の暗号通信と、端末21-mと端末31-2の暗号通信とは共通のセッション鍵で暗号化される。端末21-1と端末31-1との通信を行う場合には暗号ゲートウェイ装置180-1と180-2とを介さない伝送路を用いて通信を行う。

## 【0005】

【発明が解決しようとする課題】ところで、上述した従来の暗号通信システムにあつては、以下に示す問題点があった。第1の問題点は、インターネットというオープンなネットワークに於いて、データの転送を行う場合、第3者にデータをモニタされる可能性が高く、重要なデータの転送を容易に行うことができない。その理由は、現状使われている暗号化方式である公開鍵暗号方式を使用したとき、アルゴリズムが公開されているため、暗号を解くことは困難であるが不可能ではないからである。

【0006】第2の問題点は、秘密鍵暗号化方式を使用した場合、暗号化する際どの秘密鍵を使用してデータを転送するかの、事前了解が必要であるので、データを転送するまでに時間がかかってしまう。

【0007】そこで本発明は、既存の端末のハードウェア及びアプリケーションプログラムに影響を与えることなく機密性の高い暗号化通信を実現する暗号ゲートウェイ装置を提供することを目的としている。

## 【0008】

【課題を解決するための手段】この目的達成のため、本発明による暗号ゲートウェイ装置は、送信端末からの情報を受信し、その受信情報の暗号化／復合を行う暗号ゲートウェイ装置であつて、送信端末及び受信端末の識別情報と暗号化又は復合のためのセッション鍵の組を保持するセッション鍵テーブルと、このセッション鍵テーブルから該当するセッション鍵を検索するセッション鍵検索手段と、暗号化を行うための確認データ等を送受信するデータ送信手段及びデータ受信手段と、暗号データや

確認データ等を解析するデータ解析手段と、受信した暗号化データ又は通常データを暗号化又は復合する暗号化／復合手段と、暗号化を解く鍵データをダイヤルアップ等により別ルートにて受け渡しするための鍵データ送信手段及び鍵データ受信手段と、受信した鍵データを解析する鍵データ解析手段と、セッション鍵検索の結果で鍵データを作成する鍵データ作成手段とを備え、ユーザからの暗号化指示により、暗号化データと鍵データを物理的に別ルートで転送することを特徴とする。

【0009】この構成によれば、暗号化データと、その暗号を解くための鍵データとが物理的に異なるルートで転送されるので、機密性の高い通信を実現できる。また、送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。

【0010】

【発明の実施の形態】以下、本発明の実施の形態を、図面例と共に説明する。図1は本発明に係る暗号ゲートウェイ装置の実施の形態を用いた暗号通信システムの構成図、図2は本実施の形態の暗号ゲートウェイ装置の構成

を示すブロック図である。

【0011】図1において、暗号ゲートウェイ装置1、2はインターネット3とローカルエリアネットワーク4、5との間に設置されている。また、暗号ゲートウェイ装置4、5はダイヤルアップのために公衆網6とも接続される。暗号ゲートウェイ装置1、2は、送信側の端末（例えば端末7）から送信された情報を受信し、その受信情報を暗号化又は復合し、この結果得られた送信情報を受信側の端末（例えば端末8）へ送信して暗号通信を行うものであり、送信及び受信する情報と鍵に関する情報とが物理的に別ルートで伝達する構成になっている。

【0012】暗号ゲートウェイ装置1、2の夫々は、図2に示すように、送信側の端末から送信されるデータを受信するデータ受信手段11と、送信側の端末から受けた暗号化指示に対して暗号化指示と転送データを識別するデータ解析部12と、暗号化及び復合のためのセッション鍵の組を保持するためセッション鍵テーブル13と、選択された鍵を使用しデータの暗号化及び復合を行う暗号化／復合部14と、暗号化及び復合されたデータを送信するデータ送信手段15と、送信側の端末からの送信指示により選択された鍵を通信相手側の暗号化ゲートウェイ装置に送信するための鍵データを作成する鍵データ作成部16と、作成された鍵データを送信する鍵データ送信手段17と、鍵データを受信する鍵データ受信手段18と、受信した鍵データを解析する鍵データ解析部19と、受信した鍵データの解析結果及び送信する鍵の検索を行うセッション鍵検索部20とを備えている。

【0013】なお、上記データ受信手段11、データ送信手段15、鍵データ送信手段17及び鍵データ受信手

段18は送受信制御部21を構成する。暗号化ゲートウェイ装置4、5では暗号化／復合が自動的に行われるので、送信者は暗号化指示を行いデータを原文のまま送信し、受信者は受信したデータをそのまま利用できる。したがって、受信側では端末に暗号化通信による特別な用意をする必要はない。

【0014】次に、上記構成による暗号ゲートウェイ装置1、2の動作について説明する。図3は暗号ゲートウェイ装置1、2の動作を示すフローチャートである。なお、この説明において、ローカルエリアネットワーク4の端末7が送信側で、ローカルエリアネットワーク5の端末8が受信側とする。

【0015】暗号ゲートウェイ装置1がデータを受信したとき（ステップS200）、受信ポートの確認を行い（ステップS201）、LANポートである場合、送信側の端末7からのデータであることが判る。送信側の端末7からのデータは、暗号化指示データ若しくは通常データであるため、暗号化指示データであるか否かの判断（ステップS202）を行う。暗号化指示データであると判断した場合、送信先ネットワークの暗号ゲートウェイ装置2へ暗号化データを送信できるかを問い合わせる（ステップS203）。暗号化の問い合わせを行った後、相手からダイヤルアップ番号が取得できたか否かの判断（ステップS204）を行い、取得できた場合、問い合わせOKであり、暗号化の準備を行う。これに対し、ダイヤルアップ番号の取得ができなかった場合は送信端末側に暗号化NGの報告を行う（ステップS209）。

【0016】ダイヤルアップ番号の取得ができると、セッション鍵の検索を行い（ステップS205）、この検索が完了すると、暗号鍵の作成を行い（ステップS206）、取得したダイヤルアップ番号へ暗号鍵を送信する（ステップS207）。また、それと同時に送信側の端末7からのデータを暗号化するため、暗号化／復合部14へ暗号式の設定を行う（ステップS208）。

【0017】送信側の端末7から受け取るデータが暗号化指示データでない場合、通常データであるため、そのデータが暗号化の必要なデータであるか否かの判断を行い（ステップS210）、暗号化が不必要な場合は原文のまま送信する（ステップS211）。暗号化が必要な場合はセッションの確認を行い（ステップS212）、さらに設定されている暗号化式にて暗号処理を行い（ステップS213）、インターネット3へ送信する（ステップS214）。

【0018】一方、データ受信ポートがインターネットポートである場合、そのデータが暗号化問い合わせデータであるか否かの判断を行う（ステップS215）。暗号問い合わせデータである場合、ダイヤルアップ番号を問い合わせしてきた暗号化ゲートウェイに対して応答を行う（ステップS216）。インターネットポートから受信したデータは暗号化問い合わせデータ、暗号化データ、通

常データの三つが考えられる（ステップS 2 1 5、2 1 6）。

【0 0 1 9】インターネット3から受信したデータが暗号化問い合わせデータでない場合、暗号化データまたは通常データが考えられる、通常データは、通常のゲートウェイとして原文のままLANポートへ出力する（ステップS 2 2 0）。暗号化データを受信した場合はセッションの確認を行い（ステップS 2 1 8）、さらに設定されている復合化式により復合処理を行い（ステップS 2 1 9）、復合処理が完了した後にLANポートへ出力する（ステップS 2 2 0）。受信したポートがダイヤルアップポートである場合、鍵データの解析を行い（ステップS 2 2 1）、さらにセッション鍵の検索を行う（ステップS 2 2 2）。そして、セッション鍵の検索後、暗号化／復合部1 4にて復合処理（ステップS 2 2 3）を行う。

【0 0 2 0】次に、図4は図1を詳細に示したものであり、この図を参照してローカルエリアネットワーク4の端末7からローカルエリアネットワーク5の端末8へインターネット3を使用して暗号化データを送る場合の動作について説明する。なお、説明の都合上区別し易いように、暗号ゲートウェイ装置1にはその各部の符号に”A”を付加し、暗号ゲートウェイ装置2にはその各部の符号に”B”を付加する。

【0 0 2 1】送信側の端末7から暗号ゲートウェイ装置1の送受信制御部2 1 Aに暗号指示データが送出される。送受信制御部2 1 Aで受け取った暗号指示データはデータ解析部1 2 Aにて解析が行われ、暗号指示データであるため、インターネット3を経由してローカルエリアネットワーク5側の暗号化ゲートウェイ装置2の送受信制御部2 1 Bへ暗号化問い合わせデータを送信する。

【0 0 2 2】暗号ゲートウェイ装置2の送受信制御部2 1 Bは、問い合わせの応答としてダイヤルアップ番号をインターネット3を通して暗号ゲートウェイ装置1の送受信制御部2 1 Aへ送信する。暗号ゲートウェイ装置1の送受信制御部2 1 Aはダイヤルアップ番号を受け取ると、セッション鍵検索部2 0 Aにてセッション鍵テーブル1 3 Aを参照し、セッション鍵の検索を行う。そして、セッション鍵が決定すると、鍵データ作成部1 6 Aにて鍵データが作成され、送受信制御部2 1 Aに鍵データが渡される。

【0 0 2 3】送受信制御部2 1 Aで鍵データであると認識されると、送受信制御部2 1 Aは先に通知されているダイヤルアップ番号へ公衆網6を使用し、鍵データを送信する。また、これと同時にセッション鍵検索部2 0 Aは暗号化／復合部1 4 Aに暗号式の設定を行う。送受信制御部2 1 Aは受け取った鍵データを鍵データ解析部1 6 Aにて解析し、セッション鍵検索部2 0 Aがセッション鍵テーブル1 3 Aを参照し、暗号化／復合部1 4 Aへ復合式を設定する。

【0 0 2 4】送信側の端末7から暗号化対象のデータが暗号ゲートウェイ装置1の送受信制御部2 1 Aへ送信されると、データ解析部1 2 Aにてセッションの解析が行われ、暗号化の対象データと判断されると、暗号化／復合部1 4 Aにて暗号化され、送受信制御部2 1 Aからインターネット3を使用しデータ送信される。暗号データを受け取った暗号ゲートウェイ装置2では、データ解析部1 2 Bでセッションの解析が行われ、暗号化／復合部1 4 Bにて復合される。復合されたデータは送受信制御部2 1 Bから受信側の端末8へ送信され、受信側の端末8にて受け取られる。

【0 0 2 5】このように、この実施の形態では、ローカルエリアネットワーク4、5とインターネット3の境界に暗号ゲートウェイ装置1、2が置かれ、インターネット3を通る間だけ暗号化したデータにて転送を行い、鍵データは公衆網6のルートで転送する。したがって、暗号化データと、その暗号を解くための鍵データとが物理的に異なるルートで転送されるので、機密性の高い通信を実現でき、また送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。なお、上記実施の形態では、鍵データを公衆網6を介して転送するようにしたが、図5に示すように専用の回線9を介して転送するようにしても良い。

【0 0 2 6】

【発明の効果】本発明によれば、鍵データを公衆網又は専用回線を使用し、暗号化データと同じルートで送信しない手順を踏むようにしているので、オフライン処理を必要とせず、秘密鍵暗号化方式を使用することができる。また、暗号ゲートウェイ装置で暗号化／復合処理を行うようにしたので、セキュリティに不安のあるインターネット上での機密性を保つことができる。また、送信先の端末に特別な改造をすることなく暗号化通信ができるので、機密性保持のためのコストの上昇を最小限に抑えることができる。

【図面の簡単な説明】

【図1】 本発明に係る暗号ゲートウェイ装置の実施の形態を用いた暗号通信システムの構成図である。

【図2】 実施の形態の暗号ゲートウェイ装置の構成を示すブロック図である。

【図3】 実施の形態の暗号ゲートウェイ装置の動作を示すフローチャートである。

【図4】 図1の暗号通信システムの詳細な構成を示すブロック図である。

【図5】 本発明に係る暗号ゲートウェイ装置の他の実施の形態を用いた暗号通信システムの構成図である。

【図6】 従来の暗号通信システム（その1）の構成を示すブロック図である。

【図7】 従来の暗号ゲートウェイ装置の構成を示すブロック図である。

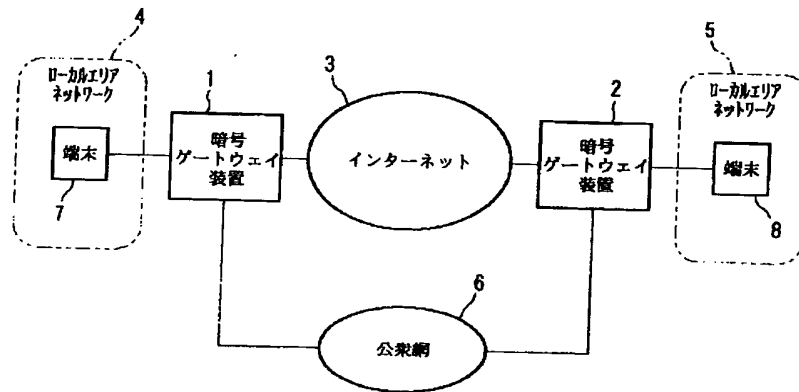
【図8】 図7の暗号ゲートウェイ装置を用いた暗号通信システム（その2）の構成を示すブロック図である。

【符号の説明】

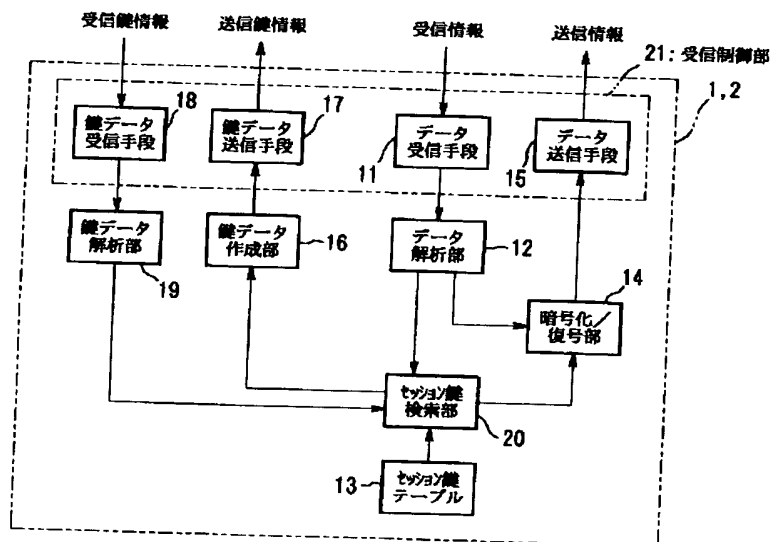
- 1、2 暗号ゲートウェイ装置
- 3 インターネット
- 4、5 ローカルエリアネットワーク
- 6 公衆網
- 7、8 端末
- 9 専用回線
- 11 データ受信手段

- \* 12 データ解析部
- 13 セッション鍵テーブル
- 14 暗号化／復号部
- 15 データ送信手段
- 16 鍵データ作成部
- 17 鍵データ送信手段
- 18 鍵データ受信手段
- 19 鍵データ解析部
- 20 セッション鍵検索部
- \* 10 21 送受信制御部

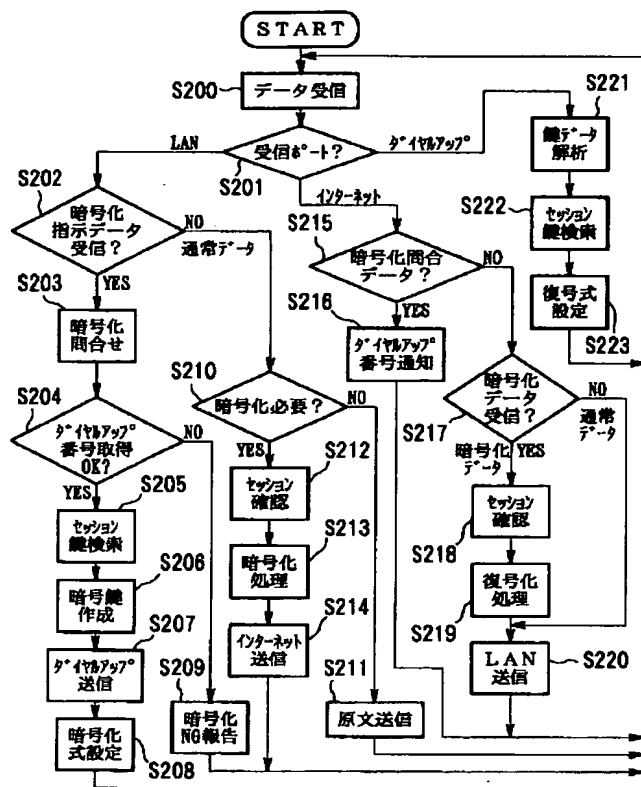
【図1】



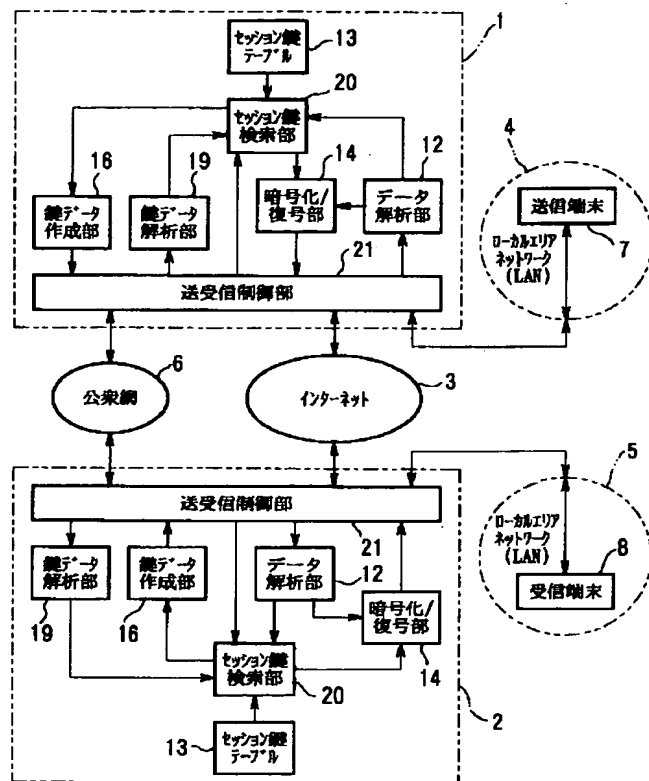
【図2】



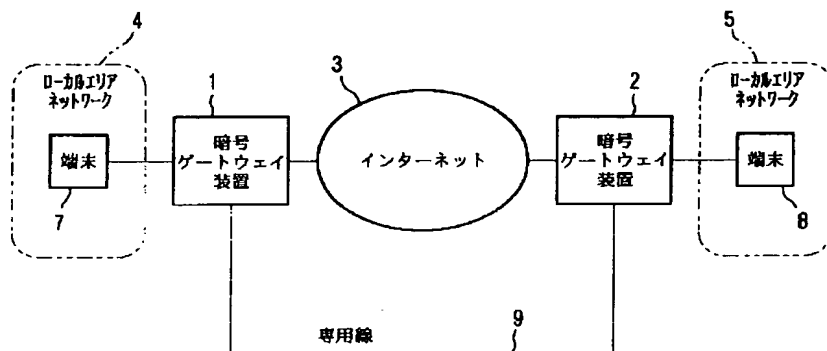
【図 3】



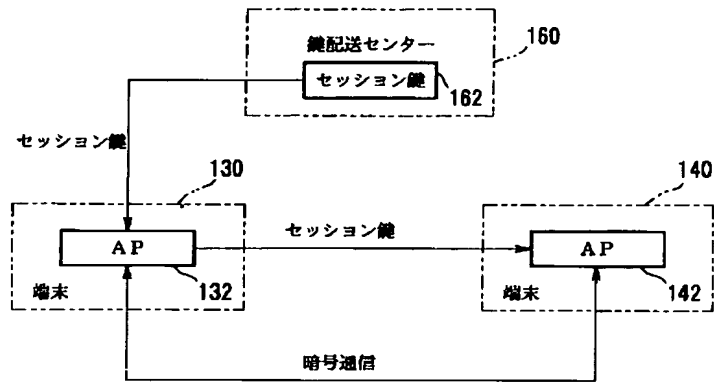
【図 4】



【図 5】

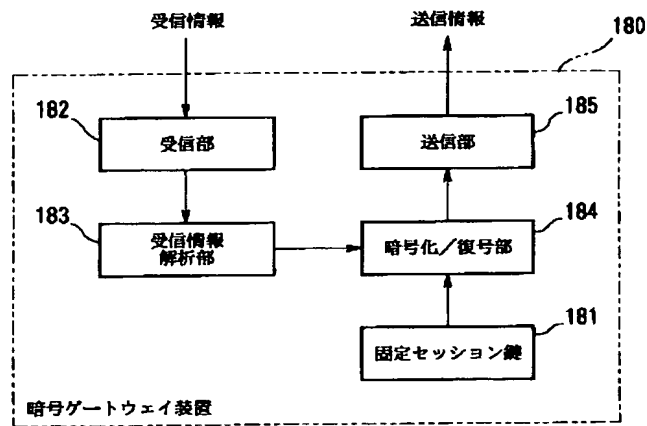


【図 6】



従来技術 (1)

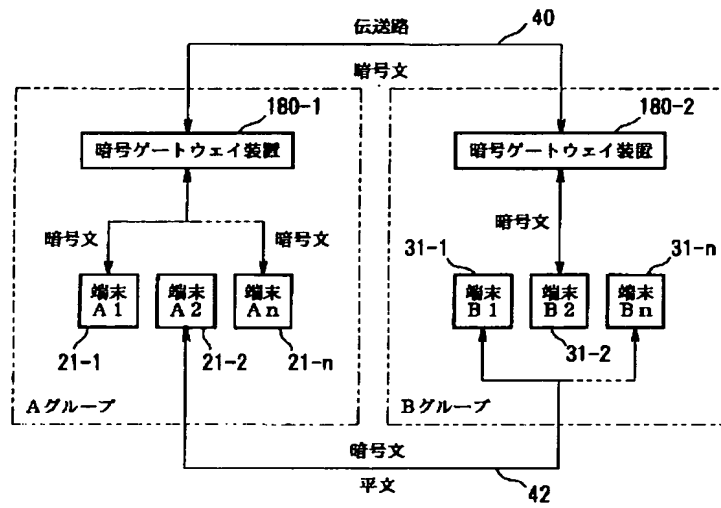
【図 7】



従来技術 (2)



【図 8】



従来技術 (2)